CSO
Custom Solutions Group

WHITE PAPER

Less Secure Than You Think

Advanced targeted attacks are growing in intensity and sophistication. Despite this reality, many organizations are far from adequately protected.

EXECUTIVE SUMMARY

This white paper examines the changing threat landscape, how the nature of security threats has evolved, and the potential financial impact across vertical markets and organizations of all sizes. This paper will explain why advanced targeted attacks have been extremely effective at breaking through traditional network security and enabling the massive data breaches and intellectual property thefts that are keeping CISOs awake at night.

The $20 Billion IT Security Hole

It's time for a security wake-up call. When it comes to advanced targeted attacks, is your organization really as protected as you want to believe?

The short answer is: probably not. Advanced targeted attacks are more sophisticated and professional than ever before, and the pace of these threats continues to accelerate. Using highly insidious techniques, cybercriminals have become extremely effective at breaking through traditional security defenses to enable massive data breaches, stealing intellectual property (IP) and enterprise credentials.

In recent years, high-level hacking schemes and cyber terrorism operations such as GhostNet, Night Dragon, and Nitro have targeted global corporations and governments to steal sensitive data, cause financial loss, and damage corporate reputations. And it's a global phenomenon: Computer spyware was said to become a weapon in the Syrian conflict in early 2012, with the government using malware that spies on opposition activists and infects their computers with viruses.

The nature of threats is changing from broad and scattershot to advanced, targeted, and persistent. Like the Operation Aurora attack on Google, or the breaches on RSA, World Bank, and Global Payment Systems that targeted IP, advanced persistent threats (APTs) use multiple stages and avenues to penetrate the network and access valuable data.

FireEye™

Malware can hide or cloak itself using techniques such as polymorphism or obfuscation. It targets unknown vulnerabilities via so-called "zero-day" attacks. Advanced targeted attacks also incorporate decades-old but highly damaging methods such as "spear phishing," where victims' personal data obtained from public social networking profiles is used to fool them into revealing sensitive information and network access credentials.

Despite an estimated $20 billion invested annually in IT security globally, according to Gartner research, a gaping security hole still exists. Case in point: Respondents to *CSO* magazine's 2012 "Global State of Information Security Survey" indicate that the threat of APTs drives their organization's security spending, but only 16 percent say their company has a security policy that addresses APTs.

APTs have become a tremendous financial liability impacting the shareholder bottom line. The problem is so serious that the U.S. Securities and Exchange Commission has issued guidance on public disclosure about cyber incidents.

The level of compromise is significant. For instance, over 95 percent of deployments see at least 10 incidents per week per Gbps, with the median about 450 incidents per week per Gbps. This is according to statistics collected from the FireEye customer base where other security devices have been deployed. The consistency in infection rate has proven the point that existing security devices are unable to catch these advanced threats. These traditional security mechanisms can no longer keep up with the highly dynamic, multi-stage attacks that have become common today with advanced targeted attacks.

"The statistic should be a wake-up call to enterprises," says Ashar Aziz, founder, CEO, and CTO, FireEye Inc., Milpitas, Calif. "They need to closely examine their current IT defense perimeter and see if advanced malware is entering their networks unimpeded, and [then] determine if they need to add an extra layer of defense to cover this harmful and costly security gap."

Coping with APTs is a CISO's nightmare. For example, 71 percent of surveyed IT security professionals believe the "changing/evolving nature of threats" is a major challenge or challenge, according to a 2011 Forrester Research report. [Source: Forrsights: "The Evolution Of IT Security, 2010 To 2011," Forrester Research Inc., February 15, 2011, Jonathan Penn and Heidi Shey.]

Security Preparedness

Typically, organizations employ a multilayered security strategy with a variety of network-based and host-level controls. This results in a false sense of security. For instance, more than 46 percent of respondents say they rely on a multilayered security program and do not believe they are currently compromised in any way, according to the IANS Data Compromise Awareness Study, February 2012. Yet FireEye research shows more than 95 percent of organizations have advanced malware infections in their Web, email, and file sharing infrastructures.

Advanced malware and targeted attacks easily evade traditional defenses such as firewalls, intrusion prevention systems (IPS), anti-virus software, and Web/email gateways. These four technologies function as the main pillars of most organizations' security framework. But alone or even as combined solutions, they cannot effectively combat advanced targeted attacks. Let's examine why.

Firewalls, which shield systems and services that should not be generally accessible, are completely blind in terms of preventing targeted and zero-day malware attacks. Both the initial attacks and subsequent malware that compromise computer systems use communication protocols that must be allowed to pass through the firewall. Next-generation firewalls (NGFW) add layers of policy rules based on users and applications, and consolidate traditional protections such as anti-virus and IPS; however, they do not add dynamic protection that can detect and block fast-changing, next-generation threats or behavior.

Intrusion prevention systems were built to detect and analyze network services-based attacks on the OS and server applications, rather than the client-side application attacks that dominate the current landscape. They use signatures, packet inspection, DNS analysis, and heuristics, but do not detect anything unusual in a zero-day exploit, especially if the malicious code is heavily disguised or delivered in stages.

Anti-virus software relies on very large databases of known threats maintained by software vendors. If the signature of a threat is identified on a system file, that file can then be quarantined or removed. But since vendors don't know about threats in advance, it's difficult to prevent them; nor can they keep pace with the volume of vulnerabilities in the various browser plug-ins. In the case of email spam filtering, where spoofed phishing sites use dynamic domains and URLs, blacklisting lags behind criminal activities. It often requires more than two days to shut down the average phishing site.

Web gateways use lists of "known bad" URLs, preventing the transmissions of Web data and websites identified as malicious. They do not protect against unknown future threats. Web filters will let a website pass with a clean reputation if the malware and vulnerability that it exploits are unknown.

Conventional network defenses are still essential, but they do not protect against advanced malware, zero-day, and targeted APT attacks because they are built on two fundamental protection technologies—lists and signatures. They only scan for the first move or the inbound attack and rely on signatures and known patterns of misbehavior to identify and block threats.

However, the most severe and successful attacks are those that exploit unknown vulnerabilities. If attacks remain below the radar, the malware is completely missed, and the network remains vulnerable to treacherous APT polymorphic code attacks that counterbalance traditional defense systems. Traditional tools may allow entry to even the most malicious code if they haven't seen it before.

Heuristics-based filtering techniques, essentially educated guesses based on behaviors or statistical correlations, also fall short. An aggressive heuristic detection policy may generate a huge number of false positives; less aggressive heuristic detection may decrease false alarms but adds the increased risk of missing malware incidents.

Deploy Dynamic Defenses to Stop Targeted, Zero-Day Attacks

"Organizations worldwide will need to augment their defenses to address the dynamic nature of today's malware that is extremely successful at penetrating today's networks," says Aziz of FireEye. "Advanced threats use a multi-stage infection cycle to maximize their chances to evade detection and successfully steal confidential information—particularly user credentials and intellectual property data."

Organizations cannot afford the potential financial, operational, and reputation risks APTs pose. Defending corporate networks from the malware used in advanced targeted attacks requires comprehensive coverage to protect against multi-vector, multi-staged attacks. Consider two examples:

- ✓ **GOVERNMENT AGENCY.** A U.S. national laboratory, which handles a huge portfolio of national secrets and sensitive data, must be able to continually enhance the effectiveness of protection against escalating global cyber threats such as advanced malware, zero-day, and targeted APT attacks. By deploying the FireEye Malware Protection System (MPS), this national agency was able to do just that and stay ahead of advanced malware. The benefits: A dramatic increase in speed of threat detection, notification, and resolution, and increased productivity without additional network or security management overhead.

The New Threat Paradigm: Multi-Vector, Multi-Stage Attacks

Advanced targeted attacks are complex, cutting across multiple threat vectors to maximize the chances of breaking through network defenses. Multi-vector attacks are typically delivered via the Web or email. They leverage application or operating system vulnerabilities, exploiting the inability of conventional network-protection mechanisms to provide a unified defense. As soon as one vulnerability is detected, Web-based attacks quickly shift to another.

The five stages of the attack lifecycle are as follows:

STAGE 1: SYSTEM EXPLOITATION. The attack attempts to set up the first stage, and exploits the system using "drive-by attacks" in casual browsing. It's often a blended attack delivered across the Web or email threat vectors, with the email containing malicious URLs, a PDF or office document.

STAGE 2: MALWARE EXECUTABLES ARE DOWNLOADED AND LONG-TERM CONTROL ESTABLISHED. A single exploit translates into dozens of infections on the same system. With exploitation successful, more malware binaries—key loggers, Trojan backdoors, password crackers, and file grabbers—are then downloaded. This means that criminals have now built long-term control mechanisms into the system.

STAGE 3: MALWARE CALLS BACK. As soon as the malware installs, attackers have cracked the first step to establishing a control point from within organizational defenses. Once in place, the malware calls back to criminal servers for further instructions. The malware can also replicate and disguise itself to avoid scans, turn off anti-virus scanners, reinstall missing components after a cleaning, or lie dormant for days or weeks. By using callbacks from within the trusted network, malware communications are allowed through the firewall and will penetrate all the different layers of the network.

STAGE 4: DATA EXFILTRATION. Data acquired from infected servers is exfiltrated via encrypted files over a commonly allowed protocol, such as FTP or HTTP, to an external compromised server controlled by the criminal.

STAGE 5: MALWARE SPREADS LATERALLY. The criminal works to move beyond the single system and establish long-term control within the network. The advanced malware looks for mapped drives on infected laptops and desktops, and can then spread laterally and deeper into network file shares. The malware will conduct reconnaissance: It will map out the network infrastructure, determine key assets, and establish a network foothold on target servers.

✓ **PROFESSIONAL SERVICES.** A large New York-based law firm must protect the interests of its financial service and multinational corporate clients. To prevent potential leaks of highly sensitive data, the firm needed a next-generation solution that would elevate its security infrastructure beyond levels provided by traditional signature-based technologies and firewall products. The solution: The FireEye Web MPS appliance, which has provided sophisticated, real-time malware protection capabilities.

Another example is Heartland Payment Systems, one of the largest payment processors in the United States. For Heartland, protection of customer data is business critical. The company learned from experience that network infiltrators had been conducting malicious activity for a while before its well-publicized breach was discovered.

"The biggest problem we face is not knowing what we don't know," says CSO John South. "We were looking for mechanisms that would find the advanced types of threats that are out there today."

FireEye has also helped Equifax, a U.S.-based consumer credit-reporting agency, find new security threats other vendors could not. Tony Spinelli, SVP and CSO of Equifax, says, "We have this category that Equifax calls unhandled malware, [with] which traditional security approaches haven't been very helpful. Putting in FireEye has really helped us detect this unhandled malware, then gives us the capability to take action to stay secure."

He continues, "The zero-day and targeted attacks that evade some of the simpler defenses are where you are going to need a next-generation product like FireEye. We looked at two or three other vendors in this space, but when we put FireEye up against the other two vendors, by far, FireEye detected and kept us secure from these issues."

A shift in the protection paradigm is a business imperative. Instead of reactive solutions that rely on known vulnerabilities, organizations require dynamic defense systems that can accurately analyze network traffic to counter advanced threats in real time. Protection must also function across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers, and plug-ins such as Flash.

"We have this category that Equifax calls unhandled malware, [with] which traditional security approaches haven't been very helpful. Putting in FireEye has really helped us detect this unhandled malware, then gives us the capability to take action to stay secure."

—Tony Spinelli, SVP and CSO, Equifax

The FireEye Approach

FireEye is the leader in stopping advanced targeted attacks that use advanced malware, zero-day exploits, and advanced persistent threat (APT) tactics. The FireEye solutions supplement traditional and next generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks.

The FireEye Malware Protection System (MPS) is the only complete solution to stop advanced targeted attacks across all threat vectors. With Web and email security to stop malware-in-motion and file security to stop malware-at-rest, the FireEye MPS offers a context-aware security solution to stop advanced attacks, mitigating the threat of APTs and enabling rapid incident response. Each of FireEye's products features a Virtual Execution (VX) engine that provides state-of-the-art, signature-less analysis using the most sophisticated virtual machines to provide a 360-degree view of each advanced attack stage, from the initial exploit and malware callback to data exfiltration. This completely integrated and proven solution is why companies around the globe choose FireEye to protect their networks against advanced targeted attacks. ■

CSO Custom Solutions Group

FireEye™

For more information, please visit
www.fireeye.com